UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/875,446	06/05/2001	Davin J. Fifield	43576.830012.US1	5057

7590 06/26/2009

Brian Kinnear
Holland & Hart LLP
555 Seventeenth Street
Suite 3200
Denver, CO 80202

EXAMINER	
TRAN, QUOC A	

ART UNIT	PAPER NUMBER
2176	

MAIL DATE	DELIVERY MODE
06/26/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte DAVIN J. FIFIELD and KEVIN S. KOCH

Appeal 2008-001226
Application 09/875,446
Technology Center 2100

Decided:[1] June 26, 2009

Before ALLEN R. MACDONALD, *Vice Chief Administrative Patent Judge*, ST. JOHN COURTENAY III, and DEBRA K. STEPHENS, *Administrative Patent Judges*.

STEPHENS, *Administrative Patent Judge*.

DECISION ON APPEAL

---

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, begins to run from the decided date shown on this page of the decision. The time period does not run from the Mail Date (paper delivery) or Notification Date (electronic delivery).

STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from a final rejection of claims 1-20. We have jurisdiction under 35 U.S.C. § 6(b).

We REVERSE and enter New Grounds of Rejection.

Introduction

According to Appellants, the invention is a method, product and signal for electronically signing an electronic transcript (Abstract and claims 1, 7, 8, 9, 17, and 19). Hash operations and concatenation are used to generate a representation of the contents of an electronic transcript and data (*id.*). The representation is recorded and time stamped creating a notary record which is digitally signed (*id.*). The digitally signed notary record, electronic transcript and identifying data are then bundled (*id.*).

Exemplary Claim(s)

Claims 1, 7, and 8 are exemplary claims and are reproduced below:

> Claim 1. A method for electronically signing an electronic transcript, comprising:
>
> performing a first hash operation on the electronic transcript to generate a representation of the contents of the electronic transcript;
>
> concatenating data to the representation of the contents of the electronic transcript, said data identifying a user;
>
> performing a second hash operation on the data concatenated to the representation, the second hash operation generating a representation of the contents of the electronic transcript and the data;
>
> providing for the recording and time stamping by a digital notary service of the representation of the contents of the electronic transcript and the data;

obtaining a notary record from the digital notary service of the time stamping;

digitally signing the notary record; and

forming an electronically signed electronic transcript by bundling the digitally signed notary record with the electronic transcript and with the data identifying the user.

Claim 7. A computer program product comprising:

a computer useable medium and computer readable code embodied on said computer useable medium for causing electronically signing an electronic transcript by a user, the computer readable code comprising:

computer readable program code devices configured to cause the computer to effect the performing a first hash operation on the electronic transcript to generate a representation of the contents of the electronic transcript;

computer readable program code devices configured to cause the computer to effect the concatenating data to the representation of the contents of the electronic transcript, said data identifying the user;

computer readable program code devices configured to cause the computer to effect the performing a second hash operation on the data concatenated to the representation, the second hash operation generating a representation of the contents of the electronic transcript and the data;

computer readable program code devices configured to cause the computer to effect the providing for the recording and time stamping by a digital notary service of the representation of the contents of the electronic transcript and the data;

computer readable program code devices configured to cause the computer to effect the obtaining a notary record from the digital notary service of the time stamping;

computer readable program code devices configured to cause the computer to effect the digitally signing the notary record; and

computer readable program code devices configured to cause the computer to effect the forming of an electronically signed transcript by bundling the digitally signed notary record with the electronic transcript and the data identifying the user.

Claim 8. A computer data signal embodied in a transmission medium, comprising:

a code segment including instructions for performing a first hash operation on an electronic transcript to generate a representation of the contents of the electronic transcript;

a code segment including instructions for concatenating data to the representation of the contents of the electronic transcript, said data identifying the user;

a code segment including instructions for performing a second hash operation on the data concatenated to the representation, the second hash operation generating a representation of the contents of the electronic transcript and the data;

a code segment including instructions for providing for the recording and time stamping by a digital notary service of the representation of the contents of the electronic transcript and the data;

a code segment including instructions for obtaining a notary record from the digital notary service of the time stamping;

a code segment including instructions for digitally signing the notary record; and

a code segment including instructions for forming an electronically signed electronic transcript including the digitally signed notary record, the electronic transcript, and the data identifying the user.

Prior Art

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Smithies	US 6,091,835	Jul. 18, 2000
Blake-Wilson	US 6,336,188 B2	Jan. 1, 2002

Kocher US 6,901,509 B1 May 31, 2005

Rejections

The Examiner rejected claims 1, 3-9, 11-15, 17, and 19 under 35 U.S.C. § 103(a) as being unpatentable over Smithies and Kocher.

The Examiner rejected claims 2, 10, 16, 18, and 20 under 35 U.S.C. § 103(a) as being unpatentable over Smithies, Kocher, and Blake-Wilson.

GROUPING OF CLAIMS

Appellants have grouped claims together to address the grounds of rejection. Appellants argue claims 1-20 based on the arguments set forth regarding claim 1 (App. Br. 13-22 and Reply Br. 1-3). We will, therefore, treat claims 2-20 as standing or falling with claim 1.

See 37 C.F.R. § 41.37(c)(1)(vii) ("Notwithstanding any other provision of this paragraph, the failure of appellant to separately argue claims which appellant has grouped together shall constitute a waiver of any argument that the Board must consider the patentability of any grouped claim separately.").

ISSUE

35 U.S.C. § 103(a): Claims 1-20

Appellants argue Smithies teaches concatenating data to the representation of the contents of the electronic transcript where the data identifies a user, and then digitally signing the notary record (App. Br. 15).

Appellants additionally argue Kocher does not teach or suggest performing a second hash operation on the data concatenated to the representation, the second hash operation generating a representation of the contents of the electronic transcript and the data (App. Br. 16). Instead, Appellants argue, Kocher teaches a method to hash a data file that once hashed, appends a digital signature (*id.*).

The Examiner finds Kocher teaches a certificate issuer name is hashed and then concatenated with a certificate serial number to produce the processed digital certificate (Ans. 13). The Examiner also finds Kocher teaches the certificate serial number may be hashed before concatenation (*id.*). Thus, the Examiner finds Kocher teaches concatenating the hashed issue name to the hashed or unhashed certificate serial number to produce a processed digital certificate (Ans. 14).

Issue: Have Appellants met the burden of showing the Examiner erred in finding Kocher teaches or suggests concatenating data to a representation of the contents of the electronic transcript where the data identifies a user and performing a second hash operation on the concatenated data?

FINDINGS OF FACT (FF)

Appellants' Invention

(1) An electronic document or electronic transcript can be electronically signed and certified by a signing entity (Spec. 5, ll. 17-24). The validity and authenticity of the electronically signed document can be

checked at a later time by a recipient of the electronic document (Spec. 5, ll. 17-21).

Smithies' Invention

(2) Smithies describes a "transcribing" method and system for collecting and storing data that evidences facts and circumstances of a party's electronic affirmation of a document, transaction or event (col. 1, ll. 16-26).

(3) The system includes a transcript generator module that creates a transcript object using one or more authentication policy components (APCs) and one of more functions within a function library (col. 11, ll. 47-55).

(4) The transcript generator module executes an affirmation process upon receiving a call from an application that creates or retrieves a record of a document, transaction, or statement, or executes processing to perform an event to be signed or affirmed (col. 12, ll. 3-8).

(5) To provide evidence to verify the integrity of the provisions or undertakings of the document, the transcript generator module creates a one-way hash corresponding to the contents of the document, transaction, or statement and the hash encoding created at the time of affirmation (col. 14, ll. 5-13). This process allows a comparison between a hash encoding of any later copy of the document, transaction, or statement and the hash encoding created at the time of affirmation to ensure the document, transaction, or statement has not been modified (col. 14, ll. 13-19).

Kocher's Invention

(6) Kocher discloses a method and system for providing cryptographic assurance based on ranges between data items on a list (Abstract).

(7) Preprocessing of certain data items that occurs includes hashing the certificate issuer name and concatenating the hashed data with a hashed or unhashed certificate serial number to produce a digital certificate (col. 6, ll. 40-46).

(8) The preprocessed data is converted into a set of sorted ranges (col. 6, ll. 54-55). The ranges are used as leaf nodes to construct a hash tree; the leaf nodes are combined using a hash function to form intermediate nodes and a root node; and the tree's root node is digitally signed by the tree issuer (col. 6, ll. 4-5, col. 7, ll. 29-42, and col. 8, ll. 15-20).

(9) This technique thus allows an efficient and secure method and system to securely demonstrate the presence or absence of items on a list – such as valid data certificates, revoked data certificates, bad credit card numbers, and computer executable code (col. 11, ll. 45-56).

PRINCIPLES OF LAW

Obviousness

In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. *See In re Fine*, 837 F.2d 1071, 1073 (Fed. Cir. 1988). In so

doing, the Examiner must make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). "[T]he examiner bears the initial burden, on review of the prior art or on any other ground, of presenting a *prima facie* case of unpatentability." *In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992). If the Examiner's burden is met, the burden then shifts to the Appellants to overcome the prima facie case with argument and/or evidence. Obviousness is then determined on the basis of the evidence as a whole and the relative persuasiveness of the arguments. *See id.*

ANALYSIS

35 U.S.C. § 103(a): Claims 1-20

Kocher teaches concatenation of a hashed certificate issuer name to a hashed or unhashed certificate serial number to produce a digital certificate (FF 7). The digital certificate is sorted to produce ranges that create a secure list of, for example, valid data certificates, revoked data certificates, bad credit card numbers, and computer executable code (FF 8 and FF 9). Kocher does not teach or disclose "concatenating data identifying a user to a representation of the contents of the electronic transcript" as recited in claim 1 (*See* analogous language in claims 7, 8, 9, 17, and 19). Thus, the Examiner has not indicated the reference or combination of references that teaches or suggests concatenating identifying data to a representation of electronic transcript contents. Therefore, we find the Examiner's

obviousness conclusion lacking in sufficient detail or support from any of the references.

We accordingly find the gap in the combined references to be uncomfortably wide and such gap cannot be bridged with theories or speculation. After considering the totality of the record before us, it is our view the weight of the evidence supports Appellants' contention that the Examiner has not sufficiently shown the correspondence between the claim elements and the relevant portions of the cited references to establish a prima facie case of obviousness.

Therefore, Appellants have shown the Examiner erred in finding Kocher teaches or suggests concatenating data to a representation of the contents of the electronic transcript where the data identifies a user and performing a second hash operation on the concatenated data.

CONCLUSION

Based on the findings of facts and analysis above, we conclude Appellants have met the burden of showing the Examiner erred in concluding that independent claims 1, 7, 8, 9, 17, and 19 are obvious over Smithies and Kocher. Since we have reversed the Examiner's rejection of each independent claim on appeal, we also reverse the Examiner's rejection of each associated dependent claim on appeal.

NEW GROUND OF REJECTION

35 U.S.C. § 101

Using our authority under 37 C.F.R. § 41.50(b), we reject claims 8, 19 and 20 under 35 U.S.C. § 101 as being directed to non-statutory subject matter.

We find that independent claims 8 and 19 both recite "a computer data signal embodied in a transmission medium."

"A transitory, propagating signal is not a 'process, machine, manufacture, or composition of matter.' Those four categories define the explicit scope and reach of subject matter patentable under 35 U.S.C. § 101." *In re Nuijten*, 500 F.3d 1346, 1357 (Fed. Cir. 2007) *reh'g and reh'g en banc denied* 515 F.3d 1361 (Fed. Cir. 2008), *cert. denied* 129 S.Ct. 70 (2008). "If a claim covers material not found in any of the four statutory categories, that claim falls outside the plainly expressed scope of § 101 even if the subject matter is otherwise new and useful." *Id.* at 1354.

Thus, since claims 8, 19, and 20 are each directed to a signal, we conclude that claims 8, 19, and 20 are non-statutory under 35 U.S.C. § 101.

DECISION

The Examiner's rejection of claims 1, 3-9, 11-15, 17 and 19 under 35 U.S.C. § 103(a) as being unpatentable over Smithies and Kocher is reversed.

The Examiner's rejection of claims 2, 10, 16, 18, and 20 under 35 U.S.C. § 103(a) as being unpatentable over Smithies, Kocher, and Blake-Wilson is reversed.

In addition to reversing the Examiner's rejections of one or more claims, this decision contains new grounds of rejection pursuant to 37 C.F.R. § 41.50(b) (2007). 37 C.F.R. § 41.50(b) provides "[a] new ground of rejection pursuant to this paragraph shall not be considered final for judicial review."

37 C.F.R. § 41.50(b) also provides that Appellants, WITHIN TWO MONTHS FROM THE DATE OF THE DECISION, must exercise one of the following two options with respect to the new grounds of rejection to avoid termination of the appeal as to the rejected claims:

> (1) Reopen prosecution. Submit an appropriate amendment of the claims so rejected or new evidence relating to the claims so rejected, or both, and have the matter reconsidered by the Examiner, in which event the proceeding will be remanded to the Examiner.…
>
> (2) Request rehearing. Request that the proceeding be reheard under § 41.52 by the Board upon the same record.…

Should Appellants elect to prosecute further before the Examiner pursuant to 37 C.F.R. § 41.50(b)(1), in order to preserve the right to seek review under 35 U.S.C. §§ 141 or 145 with respect to the affirmed rejection, the effective date of the affirmance is deferred until conclusion of the prosecution before the Examiner unless, as a mere incident to the limited prosecution, the affirmed rejection is overcome.

If Appellants elect prosecution before the Examiner and this does not result in allowance of the application, abandonment or a second appeal, this case should be returned to the Board of Patent Appeals and Interferences for final action on the affirmed rejection, including any timely request for rehearing thereof.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). See 37 C.F.R. § 1.136(a)(1)(iv) (2007).

REVERSED.
37 C.F.R. § 41.50(b)

nhl

Brian Kinnear
Holland & Hart LLP
555 Seventeenth Street
Suite 3200
Denver CO 80202